(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Patentschrift**

(10) **DE 197 02 049 C 1**

(51) Int. Cl.[6]:
H 04 L 9/32
// G06K 19/073

(21) Aktenzeichen: 197 02 049.6-31
(22) Anmeldetag: 22. 1. 97
(43) Offenlegungstag: –
(45) Veröffentlichungstag der Patenterteilung: 14. 5. 98

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
International Business Machines Corp., Armonk, N.Y., US

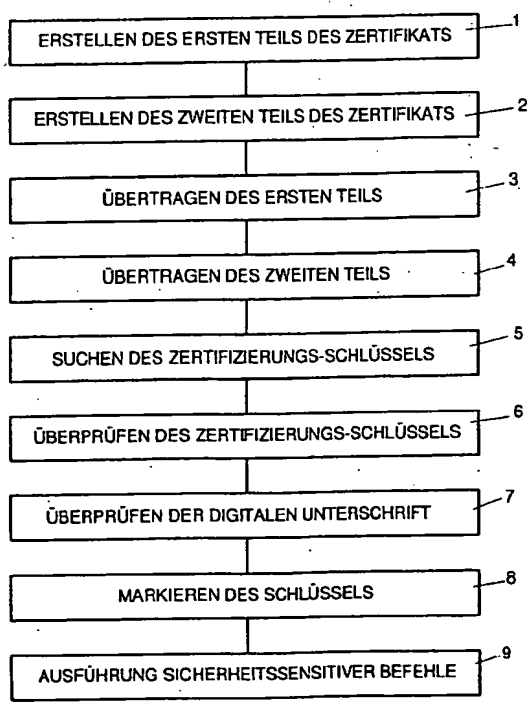
(74) Vertreter:
Rach, W., Dr., Pat.-Ass., 70569 Stuttgart

(72) Erfinder:
Deindl, Michael, Dipl.-Inform., 71034 Böblingen, DE; Hänel, Walter, Dipl.-Phys., 71088 Holzgerlingen, DE; Schaal, Albert, Dipl.-Ing., 72076 Tübingen, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
DE 32 44 537 C2
EP 03 68 596 A2
US-Z.: OMURA, J.: Novel application of Cryptography in Digital Communication, In: IEEE Communications Magazine, May 1990, S. 21-29;
DE-Z.: LEMME, H.: Chipkarten: Millardengeschäft des 21. Jahrhunderts, In: Elektronik 15, 1996, S. 56-61;
DE-B.: SCHUlte, H.: Telekommunikation, Augsburg, Interest Verlag GmbH, Stand Juni 1995, Teil. 13, Kapital 2.6, S. 6-10;
US-Z.: KÖNIGS, H.-P.: Cryptographic Identification Methods for Smart Cards in the Process of Standardization, In: IEEE Com. Magazine, June 1991, S. 42-48;

(54) Zertifizierung kryptografischer Schlüssel für Chipkarten

(57) Die Erfindung bezieht sich auf ein Verfahren zur Zertifizierung von kryptografischen Schlüsseln für Chipkarten. Hierbei werden ein Zertifizierungs-Schlüssel und ein Zertifikat auf die Chipkarte übertragen. Der erste Teil des Zertifikats umfaßt den kryptografischen Schlüssel und der zweite Teil des Zertifikats umfaßt eine digitale Unterschrift des ersten Teils des Zertifikats. Die digitale Unterschrift wird danach mittels des Zertifizierungs-Schlüssels auf der Chipkarte überprüft.



DE 197 02 049 C 1

DE 197 02 049 C 1

Beschreibung

Die Erfindung betrifft die Zertifizierung von kryptografischen Schlüsseln für Chipkarten.

Der Schutz und die Geheimhaltung von Daten in einer Chipkarte ist einer der Hauptvorteile gegenüber anderen Datenträgern, wie Magnetstreifenkarten oder Disketten. Aus diesem Grund sind eine auf diesen Zweck zugeschnittene Chiphardware und verschiedene kryptografische Verfahren notwendig.

Bei den kryptografischen Verfahren unterscheidet man symmetrische und asymmetrische kryptografische Verfahren. Im Fall der symmetrischen kryptografischen Verfahren existiert genau ein Schlüssel, der sowohl zum Verschlüsseln als auch zum Entschlüsseln der Daten verwendet wird, die mit der Chipkarte ausgetauscht werden. Dieser Schlüssel muß geheimgehalten werden, da jeder, der diesen Schlüssel kennt, Nachrichten, bestehend aus den verschlüsselten Daten, mitlesen kann. Hierdurch entsteht das Problem, wie dieser Schlüssel zwischen den Kommunikationspartnern, ausgetauscht werden kann. Über öffentliche Netzwerke ist ein Austausch des Schlüssels nicht möglich, weil der Schlüssel danach nicht mehr geheim wäre.

Dieses Problem wird teilweise mit Hilfe asymmetrischer kryptografischer Verfahren gelöst. In diesem Fall existieren ein Schlüssel V zum Verschlüsseln und ein Schlüssel E zum Entschlüsseln. Das besondere hierbei ist, daß nur einer der beiden Schlüssel geheimgehalten werden muß. Der Schlüssel V ist öffentlich bekannt und der Schlüssel E ist geheim. Will der Sender eine geheime Nachricht an einen Empfänger senden, so benutzt er den öffentlich bekannten Schlüssel V, um die Nachricht zu verschlüsseln. Wenn der Empfänger die verschlüsselte Nachricht erhält, so kann diese mit Hilfe des geheimen Schlüssels E entschlüsseln. Natürlich ist auch der umgekehrte Fall denkbar, daß der Schlüssel V geheim ist und der Schlüssel E öffentlich bekannt ist.

Aus der DE-C-32 44 537 ist ein Verschlüsselungsverfahren bekannt, bei dem kein separater Spruchschlüssel übertragen werden muß. Der zu verschlüsselnde Datenblock wir in zwei Teile aufgeteilt und aus dem ersten Teil des Datenblocks wird ein Schlüssel entnommen, mit dem ein Schlüsselrechner voreingestellt wird, wobei mit dieser Voreinstellung der zweite Teil des Datenblocks verschlüsselt wird.

Die asymmetrischen kryptografischen Verfahren lösen das Problem des Schlüsselaustausches. Es entsteht jedoch ein neues Problem. Die Authentizität des öffentlich Schlüssels muß überprüft werden. Dies geschieht, indem der öffentliche Schlüssel durch eine vertrauenswürdige Instanz zertifiziert wird. Zu diesem Zweck wird ein Zertifikat erstellt, welches die folgenden Komponenten aufweisen kann:

- einen öffentlichen Schlüssel,
- den Namen des Besitzers des öffentlichen Schlüssels,
- die Anwendungen/Anwendungsbereiche, für die dieser öffentliche Schlüssel benutzt werden darf, und
- eine digitale Unterschrift der vertrauenswürdigen Instanz.

Bei der digitalen Unterschrift handelt es sich informationstechnisch gesehen um eine Art kryptografischer Prüfsumme der übrigen Komponenten des Zertifikats ähnlich einem MAC (Message Authentication Code) über einen vorgegebenen Datenstring. Mit der digitalen Unterschrift bestätigt die vertrauenswürdige Instanz, daß die im Zertifikat enthaltenen Daten (Komponenten) zusammengehören.

Für den Aufbau und das Format eines Zertifikats existiert ein Standard X.509. Diese Norm entstand im Umfeld großer Datenbanken und setzt deshalb Computer mit großen Rechenleistungen voraus. Die Auswertung eines X.509-Zertifikates mit Hilfe eines Prozessors einer Chipkarte ist nicht möglich.

IEEE Communications Magazine, J. K. Omura, "Novel Applications of Cryptographic in Digital Communication", Mai 1990, S. 21 ff. offenbart ein Protokoll zur Verifizierung digitaler Unterschriften, wobei aus einer ersten Nachricht ein Hashwert gebildet, dann aus dem zugehörigen Entschlüsselungswert DA ein zweiter Hashwert aus der Nachricht des Senders gebildet, und schließlich die Hashwerte miteinander verglichen werden.

In H. Lemme, "Chipkarten: Milliardengeschäft des 21. Jahrhunderts", Elektronik 15 (1996), S. 56 ff. wird eine "elektronische Unterschrift beschrieben. Dies ist eine mit dem geheimen Schlüssel des Absenders verschlüsselte Prüfsumme, die sich ergibt, nachdem der zu versendende Text mit Hilfe des sogenannten "Hash-Algorithmus" komprimiert wurde. Bei jedem Dokument ergibt sich hier eine andere Zahl. Sie wird zusammen mit dem Text zum Empfänger versendet. Der wendet wieder den Hash-Algorithmus und anschließend den öffentlichen Schlüssel des Absender darauf an. Seine eigene Berechnung der Prüfsumme muß den gleichen Wert ergeben, den der Absender berechnet und übertragen hat. Auf diese Weise läßt sich Integrität der Daten prüfen.

Bei der Verwendung asymmetrischer kryptografischer Verfahren mit Chipkarten dient die Chipkarte deshalb zunächst nur zur Aufbewahrung eines Schlüssels. Die Zulassung dieses Schlüssels für das asymmetrische kryptografische Verfahren erfolgt hingegen außerhalb der Chipkarte, auf einem Computer mit größerer Rechenleistung.

Aufgabe der vorliegenden Erfindung ist es, eine verbesserte Möglichkeit zur Zertifizierung von kryptografischen Schlüsseln für Chipkarten zu schaffen.

Diese Aufgabe wird durch die in den unabhängigen Ansprüchen 1 und 17 offenbarte technische Lehre gelöst.

Der wesentliche Vorteil, welcher mit der Erfindung gegenüber dem Stand der Technik erreicht wird, besteht darin, daß eine Zertifizierung kryptografischer Schlüssel auf der Chipkarte ausgeführt werden kann. Die Funktionalität asymmetrischer kryptografischer Verfahren ist hierdurch vollständig in Chipkarten integriert. Es entsteht eine neue Stufe der Sicherheit und der Kreis möglicher Anwendungen für Chipkarten wird erweitert. Erreicht wird dies mittels eines in seiner Struktur einfachen und auf Chipkarten zugeschnittenen Zertifikats, welches in einem auf Chipkarten ausführbaren Zertifizierungsverfahren verwendet wird.

Eine Weiterbildung der Erfindung sieht vor, daß das Überprüfen der digitalen Unterschrift auf der Chipkarte die folgenden Schritte umfaßt: die Umwandlung der digitalen Unterschrift mittels des Zertifizierungs-Schlüssels, das Erzeugen eines elektronischen Fingerabdrucks des ersten Teils des Zertifikats, und das Vergleichen der umgewandelten digitalen Unterschrift mit dem elektronischen Fingerabdruck des ersten Teils des Zertifikats. Hierbei werden vorteilhaft nicht-ver-

schlüsselte Daten verglichen, jeweils verschlüsselt und entschlüsselt wird.

Zweckmäßig kann das Überprüfen der digitalen Unterschrift auf der Chipkarte die folgenden Schritte umfassen: Erzeugen eines elektronischen Fingerabdrucks des ersten Teils des Zertifikats, Umwandlung des elektronischen Fingerabdrucks mittels des Zertifizierungs-Schlüssels und einem Satz von Gleichungen, und Vergleichen des umgewandelten elektronischen Fingerabdrucks mit einem Referenzwert, welcher mit dem Zertifikat auf die Chipkarte überwiesen wird. Hierdurch wird das Ver- und Entschlüsseln eingespart, da in den Gleichungen unverschlüsselte Daten benutzt werden.

Bei einer zweckmäßigen Ausführung der Erfindung wird der kryptografische Schlüssel als ein zertifizierter Schlüssel markiert, falls beim Überprüfen der digitalen Unterschrift dieselbe als digitale Unterschrift des ersten Teils des Zertifikats verifiziert wird. Hierdurch wird sichergestellt, daß nur Schlüssel, die korrekt auf die Chipkarten übertragen wurden und korrekt in der Chipkarte abgespeichert wurden, als zertifizierte Schlüssel nutzbar werden. Im Rahmen einer Benutzung eines kryptografischen Schlüssels kann mittels der Markierung mit geringem Aufwand der Status des kryptografischen Schlüssels ermittelt werden.

Vorteilhaft kann vorgesehen sein, daß überprüft wird, ob der Zertifizierungs-Schlüssel zur Zertifizierung des kryptografischen Schlüssels benutzt werden kann. Hierdurch wird gewährleistet, daß zur Zertifizierung kryptografischer Schlüssel ausschließlich Zertifizierungs-Schlüssel verwendet werden, die vorher selbst von einer "vertrauenswürdigen Instanz" für diesen Zweck zertifiziert wurden.

Eine vorteilhafte Ausgestaltung der Erfindung sieht vor, daß der zertifizierte Schlüssel für eine Ausführung von sicherheitssensitiven Kommandos benutzt wird, wodurch der Sicherheitsstandard einer Chipkarte verbessert wird.

Zweckmäßig kann der zertifizierte Schlüssel als weiterer Zertifizierungs-Schlüssel für die Zertifizierung eines weiteren kryptografischen Schlüssels genutzt werden. Hierdurch können beliebige Zertifizierungsketten erzeugt werden.

Eine vorteilhafte Weiterbildung der Erfindung sieht vor, daß der kryptografische Schlüssel für eine Ausführung nichtsicherheitssensitiver Kommandos genutzt werden kann, nachdem das Zertifikat auf die Chipkarte übertragen wurde. Dies ermöglicht es, den kryptografischen Schlüssel bereits vor Abschluß der Zertifizierung in ausführbare Anwendungen der Chipkarte zu integrieren.

Vorteilhaft kann vorgesehen sein, daß bei einer Erzeugung der digitalen Unterschrift des ersten Teils des Zertifikats und beim Erzeugen des elektronischen Fingerabdrucks des ersten Teils des Zertifikats jeweils ein Hash-Wert mittels des Hash-Algorithmus berechnet wird. Hierdurch werden die bei der Zertifizierung zu verarbeitenden Daten komprimiert und sind anschließend im weiteren Zertifizierungsverfahren mit weniger Zeit- und Rechenaufwand zu verarbeiten.

Bei einer vorteilhaften Ausgestaltung der Erfindung kann vorgesehen sein, daß der erste und der zweite Teil des Zertifikats unabhängig voneinander auf die Chipkarte übertragen werden, wodurch ein Ausspionieren des Zertifikats erschwert wird. Weiterhin kann mit Hilfe der getrennten Übertragung die Verarbeitung des Zertifikats auf der Chipkarte effizienter gestaltet werden. Insbesondere kann ein Teil des Zertifikats offline und der andere Teil des Zertifikats online verarbeitet werden.

Eine zweckmäßige Weiterbildung der Erfindung kann dadurch gebildet sein, daß der erste Teil des Zertifikats Verwaltungsdaten umfaßt. Dies erlaubt es insbesondere, die Randbedingungen für den Einsatz und die Verwendung des kryptografischen Schlüssels festzulegen.

Bei einer zweckmäßigen Ausführung der Erfindung wird dem kryptografischen Schlüssel mittels der Verwaltungsdaten eine oder mehrere Anwendungen der Chipkarte zugeordnet, wodurch eindeutig festlegbar ist, in welchen Anwendungen der Schlüssel genutzt werden darf. Ein Mißbrauch des kryptografischen Schlüssels für andere Anwendungen wird so verhindert.

Eine vorteilhafte Ausgestaltung der Erfindung sieht vor, daß der Zertifizierungs-Schlüssel während einer Personalisierung der Chipkarte auf dieselbe übertragen wird, wodurch der Zertifizierungs-Schlüssel zusammen mit anderen sicherheitsrelevanten Daten auf die Chipkarte geladen wird.

Vorteilhaft kann vorgesehen sein, daß das Markieren des kryptografischen Schlüssels als zertifiziertem Schlüssel mittels des Setzens eines Bits in einem Status-Byte des kryptografischen Schlüssels ausgeführt wird. Das stellt eine vom Prozessor der Chipkarte leicht auswertbare Möglichkeit zur Markierung des zertifizierten Schlüssels dar.

Bei einer vorteilhaften Ausgestaltung der Erfindung kann vorgesehen sein, daß das Markieren des kryptografischen Schlüssels als zertifiziertem Schlüssel mittels einer Eintragung des kryptografischen Schlüssels in eine Tabelle auf der Chipkarte ausgeführt wird. Hierdurch können alle zertifizierten Schlüssel in einer übersichtlichen Art und Weise auf der Chipkarte gespeichert werden.

Zweckmäßig kann das Markieren des kryptografischen Schlüssels als zertifiziertem Schlüssel mittels einer Speicherung des kryptografischen Schlüssels in einem vorgesehenen Speicherbereich der Chipkarte ausgeführt werden. Um diesen kryptografischen Schlüssel später zu benutzen, bedarf es dann ausschließlich einem Verweis auf den vorgesehenen Speicherbereich.

Die abhängigen Unteransprüche des Anspruches 17 weisen die Vorteile der ihnen entsprechenden abhängigen Verfahrensansprüche auf.

Eine vorteilhafte Weiterbildung der Erfindung sieht vor, daß die Verwaltungsdaten eine Angabe eines Pfades eines Speicherbereiches auf der Chipkarte umfassen, wobei der kryptografische Schlüssel ausschließlich in diesem Speicherbereich ablegbar ist. Hierdurch kann dem kryptografischen Schlüssel ein bestimmter, besonderen Sicherheitsstandards genügender Speicherbereich auf der Chipkarte zugeordnet werden.

Ein Ausführungsbeispiel der Erfindung wird im folgenden anhand einer Zeichnung näher erläutert:

Hierbei zeigt

Fig. 1 ein Ablaufdiagramm eines Zertifizierungsverfahrens.

Zertifikate, die bei der erfindungsgemäßen Zertifizierung kryptografischer Schlüssel auf einer Chipkarte verwendet werden, weisen zwei Teile auf: Einen ersten Teil, der die eigentlichen Daten einschließlich des kryptografischen Schlüssels umfaßt, und einen zweiten Teil, die digitale Unterschrift der Daten aus dem ersten Teil.

Gemäß **Fig.** 1 wird im Verlauf eines Zertifizierungsverfahrens zunächst der erste Teil des Zertifikats erstellt. Der erste Teil weist Komponenten gemäß Tabelle 1 auf.

Tabelle 1

Komponente	Byte	Beschreibung
1	0	Bit 7 : 0 = geheimer Schlüssel 1 = öffentlicher Schlüssel Bit 6-0: Schlüsselidentifikation
2	1	Algorithmus-Identifikation
3	2	Hash-Algorithmus-Identifikation
4	3	Padding-Algorithmus-Identifikation
5	4	Nutzung Byte 0
6	5	Nutzung Byte 1
7	7	Nominelle Schlüssellänge in Bits
8	9	Länge eines Datenblocks
9	10	Länge einer Signatur
10	11	Länge der Benutzerinformation
11	12	Benutzerinformationen
12	13	Länge der Schlüsseldaten
13	15	Schlüsseldaten

Mittels der Komponente **1** des Zertifikats wird angezeigt, ob es sich bei dem zu zertifizierenden kryptografischen Schlüssel um einen öffentlichen oder einen geheimen Schlüssel handelt. Die Komponente **1** des ersten Teils des Zertifikats weist weiterhin eine Schlüsselidentifikation auf. Sie gibt erlaubte Anwendungen des im Zertifikat enthaltenen kryptografischen Schlüssels an. Soll der kryptografische Schlüssel nach Abschluß einer erfolgreichen Zertifizierung bei der Ausführung einer bestimmten Anwendung benutzt werden, so wird diese Schlüsselidentifikation erfragt und überprüft, ob der zertifizierte Schlüssel für die bestimmte Anwendung nutzbar ist. In Abhängigkeit vom Ergebnis dieser Abfrage kann der kryptografische Schlüssel anschließend entweder benutzt werden oder eine Fehlermeldung wird erzeugt.

Mit Hilfe der folgenden Komponenten **2**, **3** und **4** werden Algorithmen-Identifikationen angegeben. Komponente **2** gibt an, für welche asymmetrischen kryptografischen Verfahren der zu zertifizierende Schlüssel geeignet ist. Bei der Benutzung des zertifizierten Schlüssels können beispielhaft ein Hash-Algorithmus und/oder ein Padding-Algorithmus verwendet werden. Dies wird mit Hilfe der Komponenten **3** und **4** festgelegt. Der Hash-Algorithmus dient der Datenkomprimierung. Die Komprimierung wird ausgeführt bevor die eigentliche Ent-/Verschlüsselung stattfindet. Mittels des Padding-Algorithmus können Daten auf eine erforderliche Blocklänge aufgefüllt werden.

Mit Hilfe der Komponenten **5** und **6** können Anwendungsgebiete des kryptografischen Schlüssels festgelegt werden. Beispielhaft kann mit Hilfe der Komponente **5** bestimmt werden, daß der kryptografische Schlüssel ausschließlich zur Erzeugung elektronischen Signaturen verwendet werden darf. Die Komponente **7** gibt in Bits die Länge des kryptografischen Schlüssels an, welcher mit Hilfe des Zertifikats zertifiziert werden soll. Mit Hilfe der Komponenten **8**, **9** und **10** werden Block-Längenangaben zur Information eines Benutzers des kryptografischen Schlüssels übertragen.

Die Komponente **11** liefert Textinformationen über den kryptografischen Schlüssel. Hierbei kann es sich insbesondere um Anwendungs- oder Sicherheitshinweise für den Benutzer handeln. Die Komponente **12** gibt die eigentliche Länge des zu zertifizierenden kryptografischen Schlüssels an. Die Daten des Schlüssels befinden sich in der Komponente **13**.

Nachdem der erste Teil des Zertifikats gemäß Tabelle 1 erzeugt wurde, ist gemäß **Fig.** 1 mit der Erstellung des zweiten Teils des Zertifikats fortzufahren. Hierzu wird eine elektronische Unterschrift des ersten Teils des Zertifikats erzeugt. Eine elektronische Unterschrift dient prinzipiell zur Feststellung der Authenzitität von elektronisch übermittelten Nachrichten oder elektronischen Dokumenten. Beim erfindungsgemäßen Zertifizierungsverfahren läßt sich durch Überprüfung der digitalen Unterschrift feststellen, ob das Zertifikat ohne Veränderungen auf die Chipkarte übertragen wurde.

Der Ablauf der Erzeugung einer digitalen Unterschrift läßt sich wie folgt darstellen. Aus dem ersten Teil des Zertifikats wird mit einem Hash-Algortihmus ein Hash-Wert gebildet. Der Hash-Algorithmus dient hierbei zur Komprimierung der Daten des ersten Teils des Zertifikats. Den Hash-Wert bezeichnet man auch als Fingerabdruck der entsprechenden Daten. Anschließend wird der Hash-Wert mit einem Krypto-Algorithmus, beispielsweise dem RSA, entschlüsselt. Zur Entschlüsselung wird der geheime Schlüssel eines Schlüsselpaares, welches im jeweiligen Zertifizierungsverfahren eingesetzt wird, benutzt. Der öffentliche Schlüssel dieses Schlüsselpaares der Zertifizierungs-Schlüssel befindet sich auf der Chipkarte. Der Grund für eine Entschlüsselungsoperation bei der Erstellung einer digitalen Unterschrift liegt in der Konvention begründet, daß beim RSA-Algorithmus mit dem geheimen Schlüssel immer entschlüsselt wird und mit dem öffentlichen immer verschlüsselt wird. Das Ergebnis der Entschlüsselungsoperation ist die eigentliche Unterschrift, die Inhalt des zweiten Teiles des Zertifikats ist.

Das erfindungsgemäße Verfahren kann vorteilhaft auch mit einem beliebigen anderen Verfahren auf der Basis eines Schlüsselpaares mit geheimen und öffentlichen Schlüssel ausgeführt werden. Anwendbar sind auch Schlüsselpaare, bei deren Verwendung keine explizite Ent-/Verschlüsselung ausgeführt wird. Insbesondere Verfahren bei denen die Erfüllung einer mathematische Gleichung für die Parameter Hash-Wert, geheimer Schlüssel und öffentlicher Schlüssel Voraussetzung für die Durchführung des asymmetrischen Verfahrens ist, sind nutzbar.

Nach der Erstellung des ersten und des zweiten Teils des Zertifikats können beide auf die Chipkarte übertragen werden. Die beiden Teile des Zertifikats können zusammen oder voneinander unabhängig auf die Chipkarte übertragen werden. Getrennte Übertragungsprozesse haben den Vorteil, daß die zu übertragenden Datenmengen in den jeweiligen Prozessen geringer sind und hierdurch diese Datenmengen leichter zu verarbeiten sind.

Nachdem der erste Teil des Zertifikats in der Chipkarte gespeichert wurde, kann der darin enthaltene kryptografische Schüssel zunächst für unkritische, nicht-sicherheitssensitive Operationen auf der Chipkarte verwendet werden. Zu diesen unkritischen Operationen gehört insbesondere das einfache Überprüfen einer digitalen Unterschrift, wobei in diesem Fall das Ergebnis der Überprüfung nur an ein mit der Chipkarte kommunizierendes Gerät gemeldet wird, jedoch keine Statusänderung oder sonstige Veränderungen auf der Karte stattfinden.

Gemäß **Fig. 1** wird auf der Chipkarte in einem nächsten Schritt ein Zertifizierungs-Schlüssel gesucht. Dieser Zertifizierungs-Schlüssel ist der öffentliche Schlüssel des genannten Schlüsselpaares und muß für die Aufgabe der Zertifizierung zugelassen sein und selbst bereits zertifiziert sein. Dies bedeutet, daß er vollständig in die Chipkarte integriert sein muß. Der Zertifizierungs-Schlüssel wird vorzugsweise vom Kartenherausgeber im Rahmen der Personalisierung der Chipkarte installiert und zertifiziert. Aber auch zu einem späteren Zeitpunkt nach Abschluß der Personalisierung können Zertifizierungs-Schlüssel auf die Chipkarte aufgebracht werden. Voraussetzung ist, daß der Zertifizierungs-Schlüssel in einer Umgebung auf die Chipkarte aufgebracht wird, die entsprechenden Sicherheitsstandards genügt.

Nachdem überprüft wurde, ob der Zertifizierungs-Schlüssel für die Zertifizierung des auf die Chipkarte übertragenen Zertifikats benutzt werden darf, wird der zweite Teil des Zertifikats, welcher die digitale Unterschrift umfaßt, mit Hilfe des Zertifizierungs-Schlüssels umgewandelt. Hierbei wird die digitale Unterschrift gemäß der Konvention des RSA-Algorithmus verschlüsselt. Das Ergebnis der Berechnung ist ein Hash-Wert.

Weiterhin wird auf der Chipkarte der Fingerabdruck des ersten Teils des Zertifikats, der gleichfalls ein Hash-Wert ist, berechnet. Der Fingerabdruck wird dann mit dem Ergebnis der im vorhergehenden Abschnitt genannten Verschlüsselungsoperation verglichen. Stimmen beide überein, so wird der im Zertifikat enthaltene kryptografische Schlüssel als ein zertifizierter Schlüssel markiert.

Um die ordnungsgemäße Übertragung des Zertifikats auf die Chipkarte zu prüfen und den übertragenen Schlüssel zu zertifizieren sind auch andere kryptografischen Verfahren einsetzbar. Beispielhaft ist das bekannte DSA-Verfahren (DSA-digital signature algorithm) zu nennen. Hierbei wird mittels des geheimen Schlüssels des Schlüsselpaares und weiterer mathematischer Parameter und unter Benutzung allgemein bekannter Gleichungen ein Wert r für den ersten Teil des Zertifikats errechnet.

Nach der Übertragung des Zertifikats wird auf der Chipkarte der Wert r benutzt, um mit Hilfe weiterer bekannter Gleichungen und unter Einbeziehung des übertragenen Zertifikats und des öffentlichen Schlüssels des Schlüsselpaares einen Wert v zu berechnen. Stimmen r und v überein, wird der kryptografische Schlüssel als zertifizierter Schlüssel markiert. Auch beim DSA-Verfahren wird der Hash-Algorithmus einbezogen. Auch andere asymmetrische Verfahren können bei der Zertifizierung eingesetzt werden, wenn sie den notwendigen Sicherheitsstandard gewährleisten.

Die Markierung eines kryptografischen Schlüssel als "zertifiziert" kann insbesondere mittels des Setzens eines Bits in einem zum kryptografischen Schlüssel gehörenden Status-Byte erfolgen. Es sind jedoch auch andere Verfahren zum Markieren denkbar. Hierzu gehören das Abspeichern des kryptografischen Schlüssel in einem bestimmten Speicherbereich der Chipkarte oder das Führen einer Liste mit allen als zertifiziert markierten kryptografischen Schlüsseln.

Die Entscheidung welche Art der Markierung gewählt wird, hängt insbesondere von der Architektur der jeweiligen Chipkarte und seiner Anwendungen ab.

Nach Abschluß der Markierung des kryptografischen Schlüssels kann der zertifizierte Schlüssel für sicherheitssensitive Operationen benutzt werden. Die Markierung wird bei jedem Zugriff auf einen kryptografischen Schlüssel abgefragt. Nach Abschluß der Zertifizierung ist der zertifizierte Schlüssel zusammen mit den begleitenden Daten (siehe die Komponenten des ersten Teils des Zertifikats) auf der Chipkarte gespeichert. Die begleitenden Daten können bei jedem Zugriff auf den Schlüssel oder auch separat zur Information über den Schlüssel abgefragt werden.

Wird zur Ausführung einer sicherheitssensitiven Operation auf der Chipkarte ein zertifizierter Schlüssel benötigt, so wird der für die Operation angeforderte kryptografische Schlüssel nur verwendet, wenn seine Markierung anzeigt, daß es sich um einen zertifizierten Schlüssel handelt. Ergibt die Abfrage der Markierung ein negatives Ergebnis, d. h. es handelt sich nicht um einen zertifizierten Schlüssel, erfolgt eine Fehlermeldung. Zu den sicherheitssensitiven Operationen gehört insbesondere eine externe Authentisierung. Hierbei geht es um die Überprüfung der Identität und Authentizität eines Kommunikationspartners der Chipkarte. Die Chipkarte und ihr Kommunikationspartner (z. B. ein Terminal) stellen gegenseitig fest, ob der Kommunikationspartner ein echtes Terminal bzw. eine echte Chipkarte ist.

Ein wesentlicher Vorteil des Zertifikats gemäß Tabelle 1 ist es, daß der kryptografische Schüssel mit Hilfe der im Zertifikat enthaltenen informellen Daten einer bestimmten Anwendung zugeordnet werden kann. Dies ist insbesondere auf dem Gebiet der Chipkarten von großer Bedeutung, da hier kryptografische Schlüssel nicht individuellen Personen, sondern Anwendungen zugeordnet werden müssen. Bei diesen Anwendungen kann es sich beispielhaft um eine Gruppe von gleichartigen Geldautomaten handeln.

Die digitale Festlegung der Anwendungsgebiete im Zertifikat (vorzugsweise mittels der Komponenten **1**, **5** und **6**) erlaubt es, einen Mißbrauch des kryptografischen Schlüssels für andere Anwendungen auszuschließen.

Soll ein zertifizierter Schlüssel im Rahmen der Ausführung einer bestimmten Anwendung benutzt werden, so wird am Beginn des Zugriffs auf diesen zertifizierten Schlüssel abgefragt, ob der zertifizierte Schlüssel für die bestimmte Anwendung zugelassen ist. Dies ist mittels der zertifizierten Informationen im ersten Teils des Zertifikats möglich. Diese Informationen wurden nach der Zertifizierung zusammen mit dem kryptografischen Schlüssel in der Chipkarte gespeichert.

Werden bei Anwendungen von Chipkarten Daten einbezogen, so liegen diese in Form von Dateien vor. Diese Dateien weisen Attribute auf, welche beispielsweise vom Herausgeber der Chipkarte festgelegt werden. Die Attribute enthalten vorzugsweise einen Hinweis auf die Schlüsselidentifikation des zertifizierten Schlüssels, welcher bei einer bestimmten Operation mit den jeweiligen Dateien verwendet werden muß. Diese Schlüsselidentifikation im Attribut muß dann mit der Schlüsselidentifikation des zertifizierten Schlüssels übereinstimmen (Komponente **2** des Zertifikats). Ist dies nicht der Fall, wird die Operation nicht ausgeführt. Hierdurch wird der mißbräuchliche Gebrauch eines zertifizierten Schlüssels verhindert.

Patentansprüche

1. Verfahren zur Zertifizierung eines kryptografischen Schlüssels für eine Chipkarte, mit den folgenden Verfahrensschritten:
   a) Übertragen eines Zertifizierungs-Schlüssels auf die Chipkarte,
   b) Übertragen eines Zertifikats auf die Chipkarte, wobei ein erster Teil des Zertifikats den kryptografischen Schlüssel umfaßt und ein zweiter Teil des Zertifikats eine digitale Unterschrift des ersten Teils des Zertifikats umfaßt, und
   c) Überprüfen der digitalen Unterschrift mittels des Zertifizierungs-Schlüssels auf der Chipkarte.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß das Überprüfen der digitalen Unterschrift auf der Chipkarte die folgenden Schritte umfaßt:
   c1) Umwandlung der digitalen Unterschrift mittels des Zertifizierungs-Schlüssels,
   c2) Erzeugen eines elektronischen Fingerabdrucks des ersten Teils des Zertifikats, und
   c3) Vergleichen der umgewandelten digitalen Unterschrift mit dem elektronischen Fingerabdruck des ersten Teils des Zertifikats.
3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß das Überprüfen der digitalen Unterschrift auf der Chipkarte die folgenden Schritte umfaßt:
   c1) Erzeugen eines elektronischen Fingerabdrucks des ersten Teils des Zertifikats,
   c2) Umwandlung des elektronischen Fingerabdrucks mittels des Zertifizierungs-Schlüssels und einem Satz von Gleichungen, und
   c3) Vergleichen des umgewandelten elektronischen Fingerabdrucks mit einem Referenzwert, welcher mit dem Zertifikat auf die Chipkarte übertragen wird.
4. Verfahren nach Anspruch 1, gekennzeichnet durch einen weiteren Verfahrensschritt:
Markieren des kryptografischen Schlüssels als einen zertifizierten Schlüssel, falls beim Überprüfen der digitalen Unterschrift dieselbe als digitale Unterschrift des ersten Teils des Zertifikats verifiziert wird.
5. Verfahren nach Anspruch 1, gekennzeichnet durch einen weiteren Verfahrensschritt:
Überprüfen, ob der Zertifizierungs-Schlüssel zur Zertifizierung des kryptografischen Schlüssels benutzt werden kann.
6. Verfahren nach Anspruch 4, gekennzeichnet durch einen weiteren Verfahrensschritt:
Benutzen des zertifizierten Schlüssels für eine Ausführung von sicherheitssensitiven Kommandos.
7. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der zertifizierte Schlüssel als weiterer Zertifizierungs-Schlüssel für die Zertifizierung eines weiteren kryptografischen Schlüssels genutzt wird.
8. Verfahren nach Anspruch 1, dadurch gekennzeichnet daß der kryptografische Schlüssel für eine Ausführung nichtsicherheitssensitiver Kommandos genutzt werden kann, nachdem das Zertifikat auf die Chipkarte übertragen wurde.
9. Verfahren nach den Ansprüchen 2 oder 3, dadurch gekennzeichnet, daß bei einer Erzeugung der digitalen Unterschrift des ersten Teils des Zertifikats und beim Erzeugen des elektronischen Fingerabdrucks des ersten Teils des Zertifikats jeweils ein Hash-Wert mittels des Hash-Algorithmus berechnet wird.
10. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der erste und der zweite Teil des Zertifikats unabhängig voneinander auf die Chipkarte übertragen werden.
11. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der erste Teil des Zertifikats Verwaltungsdaten umfaßt.
12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, daß der kryptografische Schlüssel mittels der Verwaltungsdaten einer oder mehreren Anwendungen der Chipkarte zugeordnet wird.
13. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Zertifizierungs-Schlüssel während einer Personalisierung der Chipkarte auf dieselbe übertragen wird.
14. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß das Markieren des kryptografischen Schlüssels als zertifiziertem Schlüssel mittels des Setzens eines Bits in einem Status-Byte des kryptografischen Schlüssels ausgeführt wird.
15. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß das Markieren des kryptografischen Schlüssels als zertifiziertem Schlüssel mittels einer Eintragung des kryptografischen Schlüssels in eine Tabelle auf der Chipkarte ausgeführt wird.
16. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß das Markieren des kryptografischen Schlüssels als zertifiziertem Schlüssel mittels einer Speicherung des kryptografischen Schlüssels in einem vorgesehenen Speicherbereich der Chipkarte ausgeführt wird.
17. Zertifikat zum Zertifizieren eines kryptografischen Schlüssels für eine Chipkarte, mit einem ersten Teil und einem zweiten Teil, wobei die beiden Teile voneinander getrennt sind, wobei der erste Teil den kryptografischen Schlüssel umfaßt und wobei der zweite Teil eine digitale Unterschrift des ersten Teils umfaßt, dadurch gekennzeichnet, daß
das Zertifikat auf die Chipkarte übertragbar ist, und

von einem Prozessor auf der Chipkarte auswertbar ist.

18. Zertifikat nach Anspruch 17, dadurch gekennzeichnet, daß der erste Teil des Zertifikats Verwaltungsdaten umfaßt.

19. Zertifikat nach Anspruch 18, dadurch gekennzeichnet, daß
mittels der Verwaltungsdaten der kryptografische Schlüssel einer oder mehreren Anwendungen zuordenbar ist, und mittels der Verwaltungsdaten ein Mißbrauch des kryptografischen Schlüssels für andere Anwendungen, die von der einen oder den mehreren Anwendungen verschieden sind, verhinderbar ist.

20. Zertifikat nach Anspruch 18, dadurch gekennzeichnet, daß die Verwaltungsdaten eine Angabe eines Pfades eines Speicherbereiches auf der Chipkarte umfassen, wobei der kryptografische Schlüssel ausschließlich in diesem Speicherbereich ablegbar ist.

Hierzu 1 Seite(n) Zeichnungen

Numm
Int. Cl.[6]:
Veröffentlichungstag:

DE 197 02 049 C1
H 04 L 9/32
14. Mai 1998